(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

REVISED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 November 2004 (04.11.2004)

PCT

(10) International Publication Number
WO 2004/095366 A1

(51) International Patent Classification[7]: G06K 19/073, G07F 7/10, H04L 9/06

(21) International Application Number: PCT/IB2004/050478

(22) International Filing Date: 21 April 2004 (21.04.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03101094.5 22 April 2003 (22.04.2003) EP

(71) Applicant *(for all designated States except US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: PESSOLANO, Francesco [IT/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

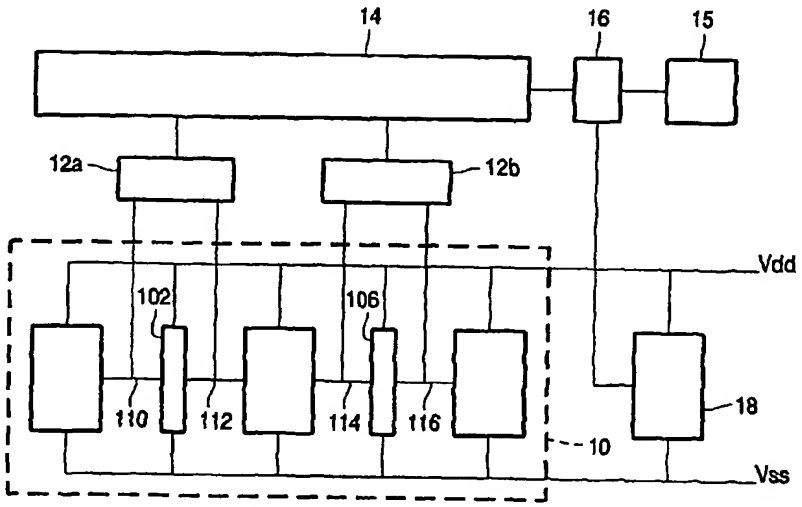
(74) Agent: ELEVELD, Koop, J.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

*[Continued on next page]*

(54) Title: ELECTRONIC CIRCUIT DEVICE FOR CRYPTOGRAPHIC APPLICATIONS




(57) Abstract: The electronic circuit executes operations dependent on secret information. Power supply current dependency on the secret information is cloaked by drawing additional power supply current. A plurality of processing circuits (102, 106) executes respective parts of the operations dependent on the secret information. An activity monitor circuit (12a, b, 14), coupled to receive pairs of processing signals coming into and out of respective ones of the processing circuits, derive activity information from each pair of processing signals. The activity monitoring circuit (12a, b, 14) generates a combined activity signal indicative of a sum of power supply currents that will be consumed by the processing circuits (102, 106) dependent on the processing signals. A current drawing circuit connected to the power supply connections is controlled by the activity monitor circuit (12a, b, 14) to draw a cloaking current controlled by the combined activity signal, so that power supply current variations dependent on the secret information are cloaked in a sum of the cloaking current and current drawn by the processing circuits (102, 106).

WO 2004/095366 A1

**Declaration under Rule 4.17:**

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

**Published:**

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

**(88) Date of publication of the revised international search report:** 9 December 2004

**(15) Information about Correction:**
see PCT Gazette No. 50/2004 of 9 December 2004, Section II

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

# INTERNATIONAL SEARCH REPORT

PCT/IB2004/050478

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/073 G07F7/10 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G07F H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 6 498 404 B1 (THUERINGER, ULLY, ARNOLD, EBER) 24 December 2002 (2002-12-24)<br>cited in the application<br>abstract; figure 2<br>column 2, line 39 - column 3, line 13 | 1-7 |
| A | DE 198 28 936 A (SIEMENS AG)<br>2 December 1999 (1999-12-02)<br>column 1, line 23 - line 30<br>column 2, line 15 - line 18 | 1 |
| A | US 6 320 770 B1 (FEUSER MARKUS)<br>20 November 2001 (2001-11-20)<br>cited in the application<br>the whole document | 1 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 12 October 2004 | 18. 10. 04 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Heusler, N |

Form PCT/ISA/210 (second sheet) (January 2004)

# INTERNATIONAL SEARCH REPORT

PCT/IB2004/050478

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 6 419 159 B1 (ODINAK GILAD)<br>16 July 2002 (2002-07-16)<br>cited in the application<br>column 3, line 31 - line 55; figure 1 | 1 |
| A | WO 00/63827 A (WEDER UWE ; INFINEON TECHNOLOGIES AG (DE))<br>26 October 2000 (2000-10-26)<br>cited in the application<br>abstract<br>page 4, line 26 - line 35 | 1 |
| A | DE 198 22 220 A (GIESECKE & DEVRIENT GMBH)<br>25 November 1999 (1999-11-25)<br>column 1, line 51 - column 2, line 30 | 1 |
| A | DE 199 07 575 A (PHILIPS CORP INTELLECTUAL PTY) 24 August 2000 (2000-08-24)<br>abstract<br>column 1, line 5 - line 28<br>column 1, line 50 - line 56<br>column 4, line 61 - line 67 | 1 |
| A | PAUL KOCHER, JOSHUA JAFFE, BENJAMIN JUN:<br>"Differential Power Analysis"[Online]<br>1 January 2000 (2000-01-01), pages 1-16,<br>XP002291002<br>SAN FRANCISCO, USA<br>Retrieved from the Internet:<br>URL:http://www.cryptography.com/dpa><br>[retrieved on 2004-08-03]<br>page 1 - page 16 | 1-7 |

# INTERNATIONAL SEARCH REPORT

PCT/IB2004/050478

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 6498404 B1 | 24-12-2002 | DE 19850721 A1 | 18-05-2000 |
| | | CN 1292111 T | 18-04-2001 |
| | | WO 0026746 A2 | 11-05-2000 |
| | | EP 1057096 A2 | 06-12-2000 |
| | | JP 2003526134 T | 02-09-2003 |
| | | TW 460774 B | 21-10-2001 |
| DE 19828936 A | 02-12-1999 | DE 19828936 A1 | 02-12-1999 |
| | | AT 227445 T | 15-11-2002 |
| | | BR 9910802 A | 13-02-2001 |
| | | CN 1303493 T | 11-07-2001 |
| | | WO 9963419 A1 | 09-12-1999 |
| | | DE 59903326 D1 | 12-12-2002 |
| | | EP 1280037 A2 | 29-01-2003 |
| | | EP 1080400 A1 | 07-03-2001 |
| | | JP 2002517787 T | 18-06-2002 |
| | | US 2003118190 A1 | 26-06-2003 |
| US 6320770 B1 | 20-11-2001 | DE 19936919 A1 | 06-04-2000 |
| | | WO 0019366 A1 | 06-04-2000 |
| | | EP 1044426 A1 | 18-10-2000 |
| | | JP 2002526839 T | 20-08-2002 |
| US 6419159 B1 | 16-07-2002 | NONE | |
| WO 0063827 A | 26-10-2000 | WO 0063827 A1 | 26-10-2000 |
| DE 19822220 A | 25-11-1999 | DE 19822220 A1 | 25-11-1999 |
| | | AU 4144399 A | 06-12-1999 |
| | | CA 2332350 A1 | 25-11-1999 |
| | | CN 1308752 T | 15-08-2001 |
| | | WO 9960534 A1 | 25-11-1999 |
| | | EP 1080454 A1 | 07-03-2001 |
| | | JP 2002516444 T | 04-06-2002 |
| DE 19907575 A | 24-08-2000 | DE 19907575 A1 | 24-08-2000 |
| | | AT 246819 T | 15-08-2003 |
| | | DE 50003153 D1 | 11-09-2003 |
| | | EP 1031903 A2 | 30-08-2000 |
| | | JP 2000253575 A | 14-09-2000 |
| | | US 6172494 B1 | 09-01-2001 |